

47

Notice of Allowability

Application No.

09/880,470

Examiner

Peter Poltorak

Applicant(s)

PERLMAN, RADIA J.

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to papers filed on 8/05/2005.
2. ☒ The allowed claim(s) is/are 1,4-7,9-23,25-28,30-33,35 and 37.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on 8/05/2005.
2. Claims 18-19, 25, 30 and 35 have been amended.
3. Claims 2-3, 8, 24, 29, 34 and 36 have been canceled.
4. Claim 37 has been added.
5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Examiner Amendment

6. An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the Issue Fee.

The following changes were authorized (and permission to make same by Authorization for this Examiner's Amendment was given in a telephone interview with Paul D. Sorkin (617.367.4600) on June 13, 2001).
7. The previous claims have been replaced with the attached version of claims.

Allowable Subject Matter

8. Claims 1, 4-7, 9-23, 25-28, 30-33, 35 and 37 are allowed.
9. The following is a statement of reasons for the indication of allowable subject matter.
10. The closest prior art: *Perlman* (U.S. Patent No. 6363480), *Hanna* (U.S. Pub. 2002/0136410 A1) and *Perlman et al.* (WO 01/20836 A2) refer to method and apparatus employing ephemeral keys.
11. However, the found art do not teach: "receiving, at a first node, a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value; decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value... wherein the first and third encryption keys are the same and the first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node" as required by claim 1.
12. The art also lacks teaching of: "communicating a proof value from a second node to said first node... determining that the second node is authorized to receive said singly wrapped value as a function of said proof value and said integrity verification key" as required by claim 18.

EXAMINER'S AMENDMENT

--

1. (Previously presented) A method of performing secure ephemeral communication comprising:

receiving, at a first node, a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

securely communicating said doubly wrapped value to a second node from the first node;

obtaining a second decryption key having a predetermined expiration time at the second node;

determining if said second decryption key has expired;

decrypting said doubly wrapped value using said second decryption key to produce said singly wrapped value if it has been determined that said second decryption key has not expired; and

securely communicating said singly wrapped value from the second node to the first node,

wherein the first and third encryption keys are the same and the first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

Claims 2 and 3: Canceled.

4. (Original) The method of claim 1 further including the step of decrypting said singly wrapped value to obtain said value using said first decryption key.

5. (Original) The method of claim 1 wherein said first encryption and decryption keys comprise a first public and private key pair.

6. (Original) The method of claim 1 wherein said second encryption and decryption keys comprise a second public and private key pair.

7. (Original) The method of claim 1 wherein said third encryption and decryption keys comprise a third public and private key pair.

8. Canceled.

9. (Previously presented) The method of claim 1 further including the steps of:
receiving, at said first node, an identifier associated with said second node; and

forwarding said doubly wrapped value to said second node at an address associated with said identifier.

10. (Original) The method of claim 9 wherein said identifier comprises a uniform resource locator associated with said second node.

11. (Previously presented) The method of claim 1 wherein said step of securely communicating said doubly wrapped value to said second node from the first node comprises the steps of:

encrypting said doubly wrapped value with a fourth encryption key to form an encrypted doubly wrapped value, wherein said fourth encryption key has a corresponding fourth decryption key;

encrypting said fourth decryption key with said second encryption key;

communicating said encrypted fourth decryption key and said encrypted doubly wrapped value from said first node to said second node;

decrypting said encrypted fourth decryption key to obtain said fourth decryption key using said second decryption key in the event said second decryption key has not expired; and

decrypting said encrypted doubly wrapped value using said fourth decryption key to obtain said doubly wrapped value,

wherein the fourth encryption and decryption keys are generated by the first node.

12. (Original) The method of claim 11 wherein said fourth encryption and decryption keys comprise symmetric keys.

13. (Previously presented) The method of claim 11 further including the steps of encrypting said fourth encryption key with said second encryption key and communicating said encrypted fourth encryption key to said second node; and wherein said step of securely communicating said singly wrapped value to the first node comprises the steps of:

decrypting said encrypted fourth encryption key using said second decryption key to obtain said fourth encryption key, in the event said second decryption key has not expired;

encrypting said doubly wrapped value with said fourth encryption key to obtain a securely wrapped value;

communicating said securely wrapped value from said second node to said first node; and

decrypting said securely wrapped value using said fourth decryption key to obtain said doubly wrapped value.

14. (Original) The method of claim 13 wherein said fourth encryption and decryption keys comprise symmetric keys.

Art Unit: 2134

15. (Previously presented) The method of claim 1 wherein said value comprises a first secret key and said method further comprises the steps of:

at a third node, encrypting information with said first secret key to form an encrypted information value;

communicating said encrypted information value from the third node to said first node;

decrypting said singly wrapped value at said first node using said third decryption key to obtain said first secret key; and

decrypting said encrypted information value at said first node using said first secret key to obtain said information.

16. (Previously presented) The method of claim 15 further including the step of deleting said first secret key at said first node subsequent to decrypting said encrypted information value.

17. (Original) The method of claim 1 further including the step of receiving at said second node a key identifier associated with said second decryption key and said obtaining step comprises the step of using said key identifier to select said second decryption key from a plurality of decryption keys accessible by said second node.

18. (Currently amended) A method of performing secure ephemeral communication comprising:

Art Unit: 2134

receiving, at a first node, a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form said doubly wrapped value;

receiving, at said first node, an integrity verification key securely associated with said doubly wrapped value;

communicating a proof value from a second node to said first node;

obtaining at said first node a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

determining if said second decryption key has expired;

decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired;

at the first node, determining that the second node is authorized to receive said singly wrapped value as a function of said proof value and said integrity verification key;

if it is determined that said second node is authorized to receive said singly wrapped value, securely communicating said singly wrapped value to said second node by encrypting the singly wrapped value with a third encryption key to form an encrypted singly wrapped value, wherein said third encryption key has a corresponding third decryption key accessible to said second node, and communicating said encrypted singly wrapped value from said first node to said second node; and

decrypting, at the second node, said encrypted singly wrapped value received from said first node using said third decryption key to obtain said singly wrapped value.

19. (Previously presented) The method of claim 18 further comprising the step of decrypting said singly wrapped value to obtain said value using a first decryption key associated with said first encryption key and accessible to said second node.

20. (Currently amended) The method of claim 19 wherein said first encryption and decryption keys comprise first public and private keys of a public-private key pair associated with said second node.

21. (Original) The method of claim 18 wherein said second encryption and decryption keys comprise second public and private keys of a second public-private key pair associated with said first node.

22. (Currently amended) The method of claim 18 wherein said integrity verification key comprises a first public key associated with said second node and said securely associating step comprises the step of encrypting said singly wrapped value and said first public key with said second encryption key, said step of communicating said proof value comprises the step of generating by said second node a digital signature using said second node private key, and said step of determining that said second ~~node~~ node is authorized to receive the singularly wrapped value comprises the step of verifying said digital signature at said first node using said second node public key.

Art Unit: 2134

23. (Previously presented) The method of claim 18 wherein said step of communicating said proof value that said second node is authorized comprises the step of securely communicating from said second node to the first node said proof value that said second node is an authorized decryption agent for said value.

24. Canceled

25. (Currently amended) The method of claim 18 wherein said third encryption and decryption keys comprise a first symmetric key pair.

26. (Original) The method of claim 19 wherein said value comprises a secret key and said method further includes the steps of:

receiving at said second node an encrypted information payload comprising an information payload encrypted with said secret key; and

decrypting said encrypted information payload at said second node using said secret key.

27. (Previously presented) A system for performing secure ephemeral communication comprising:

first, second and third communicably coupled nodes, each of said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

program code within said first node memory for receiving a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value, and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

program code within said first node memory for decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

program code within said first node memory for securely communicating said doubly wrapped value to said second node;

program code within said second node memory for obtaining a second decryption key having a predetermined expiration time at said second node, wherein said second decryption key is associated with said second encryption key;

program code for determining if said second decryption key has expired;

program code within said second node memory for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired; and

program code within said second node memory for securely communicating said singly wrapped value to the first node following decryption of said doubly wrapped value,

wherein said first and third encryption keys are the same and said first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

28. (Previously presented) The system of claim 27 further including program code within said first node memory for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.

29. Canceled.

30. (Currently amended) A system for performing secure ephemeral communication comprising:

first and second communicably coupled nodes, said nodes including a processor and a memory, the processor in each respective node being configured to execute program code contained within the respective memory;

program code within said first node memory for receiving a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form said doubly wrapped value;

program code within said first node memory for receiving an integrity verification key securely associated with said doubly wrapped value;

program code within said second node for communicating a proof value from said second node to said first node;

program code within said first node for obtaining a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

program code within said first node for determining if said second decryption key has expired;

program code within said first node memory for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired;

program code within said first node memory for determining that the second node is authorized to receive said singly wrapped value as a function of said proof value and said integrity verification key; and

program code within said first node memory for securely communicating said singly wrapped value to said second node, in response to a determination that said second node is authorized to receive said singly wrapped value, by: encrypting the singly wrapped value with a third encryption key to form an encrypted singly wrapped value, wherein said third encryption key has a corresponding third decryption key accessible to said second node; and communicating said encrypted singly wrapped value from said first node to said second node; and

program code within said second node memory for decrypting said encrypted singly wrapped value received from said first node using said third decryption key to obtain said singly wrapped value.

31. (Original) The system of claim 30 further including program code within said second node memory for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.

32. (Previously presented) A system for performing secure ephemeral communication comprising:

first, second and third communicably coupled nodes, each of said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

means associated with said first node for receiving a triply wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value, and said doubly wrapped value being encrypted with a third encryption key to form said triply wrapped value;

means associated with said first node for decrypting said triply wrapped value using a third decryption key associated with said third encryption key to obtain said doubly wrapped value;

means associated with said first node memory for securely communicating said doubly wrapped value to said second node;

means associated with said second node for obtaining a second decryption key having a predetermined expiration time, wherein said second decryption key is associated with said second encryption key;

means associated with said second node for determining if said second decryption key has expired;

means associated with said second node for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired; and

means associated with said second node memory for securely communicating said singly wrapped value to the first node following decryption of said doubly wrapped value;

wherein said first and third encryption keys are the same and said first and third decryption keys are the same and the first and third encryption and decryption keys are associated with the first node.

33. (Previously presented) The system of claim 32 further including means associated with said first node for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.

34. Canceled.

35. (Currently amended) A system for performing secure ephemeral communication comprising:

first and second communicably coupled nodes, said nodes including a processor and a memory, the processor in each respective node being operative to execute program code contained within the respective memory;

means, associated with said first node, for receiving a doubly wrapped value, said value being encrypted with a first encryption key to form a singly wrapped value, said singly wrapped value being encrypted with a second encryption key to form a doubly wrapped value;

means, associated with said first node, for receiving an integrity verification key securely associated with said doubly wrapped value;

means, associated with said second node, for communicating a proof value from said second node to said first node;

means, associated with said first node, for obtaining a second decryption key associated with said second encryption key, said second decryption key having a predetermined expiration time;

means for determining if said second decryption key has expired;

means, associated with said first node, for decrypting said doubly wrapped value using said second decryption key to obtain said singly wrapped value if it has been determined that said second decryption key has not expired;

Art Unit: 2134

means, associated with said first node, for determining that the second node is authorized to receive said singly wrapped value as a function of said proof value at first node and said integrity verification key; ~~and~~

means, associated with said first node, for securely communicating said singly wrapped value to said second node, in response to a determination that said second node is authorized to receive said singularly wrapped value, by: encrypting the singly wrapped value with a third encryption key to form an encrypted singly wrapped value, wherein said third encryption key has a corresponding third decryption key accessible to said second node; and communicating said encrypted singly wrapped value from said first node to said second node; and

means, associated with said second node, for decrypting said encrypted singly wrapped value received from said first node using said third decryption key to obtain said singly wrapped value.

36. Canceled

37. (new) The system of claim 35, further comprising:

means, associated with said second node, for decrypting said singly wrapped value using a first decryption key associated with said first encryption key.


--

Art Unit: 2134

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached from Monday through Thursday from 9:00 until 5:00, and every other Friday from 9:00 until 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-1600.


09/14/08



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100